Open Journal of Legal Science 法学, 2024, 12(9), 5574-5579
Published Online September 2024 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2024.129794

Hans汉斯

数据安全认证：政府监管下的第三方认证

王雨雨

长春理工大学法学院，吉林 长春

收稿日期：2024年7月19日；录用日期：2024年7月31日；发布日期：2024年9月11日

摘　要

数据安全认证是数据安全治理体系中的一个重要环节，具有“软法”性质的数据安全认证不仅具有公法上保护数据安全的作用，同时也具有促进数字经济繁荣发展的商业价值。传统的数据认证从政府、社会、市场三方面进行规制，但是各有利弊。欧盟《一般数据保护条例》在传统的模式上发展出了政府监管下的数据认证模式，体现了合作共治的理念。我国的数据认证制度也随着《数据安全管理认证实施规则》的出台步入正轨，应通过不断细化规则、明确认证机构责任等方式实现联动适用，对已有制度进行补充和完善。

关键词

数据安全认证，第三方认证，个人信息保护

Data Security Certification: Third-Party Certification under Government Supervision

Yuyu Wang

School of Law, Changchun University of Science and Technology, Changchun Jilin

Received: Jul. 19th, 2024; accepted: Jul. 31st, 2024; published: Sep. 11th, 2024

Abstract

Data security certification is an important part of the data security governance system, and the data security certification with the nature of “soft law” not only has the role of protecting data security in public law, but also has the commercial value of promoting the prosperity and development of the digital economy. Traditional data authentication is regulated from the government, society, and the market, but each has its own advantages and disadvantages. The EU *General Data Protection Regulation* (GDPR) has developed a data authentication model under government supervision from the traditional model, reflecting the concept of cooperation and co-governance. China’s data certification system is also on the right track with the promulgation of the *Data Security Management*

文章引用: 王雨雨. 数据安全认证: 政府监管下的第三方认证[J]. 法学, 2024, 12(9): 5574-5579.
DOI: 10.12677/ojls.2024.129794

***Certification Implementation Rules*, which should be applied in conjunction with each other by continuously refining the rules and clarifying the responsibilities of certification bodies, so as to supplement and improve the existing systems.**

Keywords

Data Security Certification, Third-Party Certification, Protection of Personal Information

1. 引言

在大数据信息飞速发展的时代，数据安全在网络信息领域的重要性日益凸显。大数据、人工智能的出现给传统的数据保护带来了一系列的挑战，如何应对新兴领域出现的数据处理与应用场景，这成为了数据保护法律规范发挥作用的重中之重。2018 年 5 月生效的欧盟《一般数据保护条例》(GDPR)正式引入了“数据认证”，不仅为企业提供了独有的公示营业价值，同时也提高了个人数据保护的能力。随着信息网络的发展，数据安全认证逐渐成为全球数据治理的重要手段。我国的数据安全认证也逐渐得到重视和发展。2019 年 7 月，国务院《关于印发中国(上海)自由贸易试验区临港新片区总体方案的通知》首次提出“建立数据保护能力认证机制”，第一次明确了数据安全认证是数据安全管理机制的重要部分。此后，我国《网络安全法》第 17 条以及《数据安全法》第 18 条第 1 款均有涉及数据安全认证的规定[1]。《个人信息保护法》第 38 条将个人信息保护认证作为向境外提供个人信息的合法性条件之一，第 62 条要求“推进个人信息保护社会化服务体系建设，支持有关机构开展个人信息保护评估、认证服务”。此外，2019 年国家市场监管总局、中央网信办发布《关于开展 App 安全认证工作的公告》，对互联网个人信息的收集及保护作出了规范。2022 年 12 月 2 日中共中央、国务院发布的《关于构建数据基础制度更好发挥数据要素作用的意见》明确了建立实施数据安全管理认证制度，引导企业通过认证提升数据安全管理水平。

2. 数据安全认证的缘起及价值

关于“认证”这一概念的界定，国际标准组织(ISO)是这样规定的：“由独立机构出具的书面保证(证书)，以证明所提供的产品、服务或系统符合特定要求。”基于此，认证也被称为“第三方合格证明”。这里的“证明”是指“发布一项声明，该声明是基于评审后认定某种产品或某项服务满足了特定要求”(ISO17000:2004) [1]。欧盟《一般数据保护条例》仅使用了“认证机制、印章和标记”的统称，并没有单独定义其中某项的具体内容。证书是对合规性的一种声明。为了欧盟内部使用数据保护标准更加清晰，欧盟数据保护理事会制定了《认证和认证标准指南》，将“数据认证”这一概念的内涵进行了明确，即“有关数据控制者及处理者的数据处理规程的第三方证明”。我国《认证认可条例》第二条对“认证”这一概念的定义是，由认证机构证明产品、服务、管理体系符合相关技术规范、相关技术规范的强制性要求或者标准的合格评定活动。由此可见，数据安全认证主要是网络信息领域通过第三方机构的评定证明处理数据，与政府的规制和企业自制不同的一种保障数据安全的“软性”约束[2]。

[1]《网络安全法》第 17 条明确要求“开展网络安全认证、检测、风险评估等安全服务”。《数据安全法》第 18 条第 1 款原则性的规定了数据安全认证：“国家促进数据安全检测评估、认证等服务的发展，支持数据安全检测评估、认证等专业机构依法开展服务活动。”

数据安全认证是大数据和网络信息发展所带来的必然趋势，与传统模式不同的评价证明机制不仅在保障数据安全上发挥重要作用，同时能带来数字经济领域上的显著质效。第一，在个人信息保护层面的保障作用能提高用户对数据处理者以及数字产业的认可与信任，同时也能为数据处理者提供便利。在网络信息繁杂的领域，存在大量不被消费者所熟知的企业，如何在数字产业获得足够的竞争力，是企业在网络市场中要考虑的关键问题。消费者的倾向大多是有足够保障的知名企业以及获得信誉认证的企业，网络认证具有独特的标记功能，它的主要特征得到普遍的认可，尤其是消费者群体，也就是那些将个人数据托付给企业家而且数据安全对其至关重要而他们又无法自行验证数据保护标准的消费者。获得了数据安全认证，也就意味着企业获得了更多被用户选择的机会，因为认证相当于数字经济市场中的信誉担保。可以有效防止互联网企业陷入自证的困局，企业在网络领域的竞争力得到保障也就有更多的精力投入提升产品品质上，实现效率质量和用户信任感的良性循环。

第二，数据安全认证能够帮助数据保护机构更好地判断数据处理是否适当，减轻监管部门的压力。数据安全认证监管部门会以公众易于访问的形式，发布用以挑选和认定认证机构的要求，以及认证机构执行的认证标准。在这种统一的标准的作用下，数据安全认证将数据保护转化为可操作的合规的程序，企业可以根据要求规范内部的合规的制度和管理体系。同时，对于那些小微企业，即使缺乏专门的数据保护人员也能通过专业的认证机构建立自己的数据保护制度，达到最基本的数据保护的要求。监管部门也能通过直观的证书或印章，进行监管与规制。

数据安全认证可以引导数据处理者提升数据安全保障能力，促进数字经济的繁荣发展。在数据安全认证的机制之下，获得确认数据处理操作合规的证书或印章，是数据处理者证明其合法性和正确性的一种方法，这在无形中相当于为数据处理者套上了无形中的“紧箍咒”。在这种引导和激励下，数据处理者会努力提高自身的数据安全保障能力以求获得认证，否则会失去相当一部分的市场竞争力。数据安全认证通过这种安全性的保障和获取的便利性可以在一定程度上提高用户网络交易的比例，促进数字产业交易和流通的多元化，有利于数字经济的协调发展。

3. 域外认证的模式与应用

(一) 域外认证的模式

数据认证在数据安全保护方面有着举足轻重的作用，那么如何确保数据安全认证有效发挥作用，数据认证的主体选择和过程的监督就显得尤为重要。从域外国家数据认证的发展状况来看，数据认证可以分为三种模式，分别是国家认证、第三方认证以及自我声明。国家认证是根据政府公布的法律和技术标准确立一系列认证规范，在“硬法”层面上对认证过程及标准施以全程监督；第三方认证是以社会治理的形式来为数据认证提供信誉支撑；自我声明则是以企业自我承诺的形式来保证自身的数据保护能力[3]。

1) 国家认证

国家认证的主要实践地区是法国和德国，两者都将数据保护机构作为数据认证的主要实施主体。法国主要由数据保护机构——国家信息与自由委员会(CNIL)来负责制定认定标准以及根据标准评估企业是否符合标准并授予认证证书。2004 年，法国《数据保护法案》修正案就允许 CNIL 为“旨在保护个人数据的产品或程序”签发隐私印章(Label CNIL)。值得注意的是，要想获得 CNIL 的印章，企业的数据处理能力所要达到的不仅仅是合规，而是要足够优秀足以成为行业典范。德国的数据认证主体是石荷州的数据保护专员(ULD)，它最早产生于 2002 年，石荷州法规定了数据保护印章这一认证的形式。石荷州数据保护印章的程序设计体现了浓厚的行政色彩，属于国家认证的典型。

国家认证的优点在于它是由公权力来进行数据安全的保障，可以保证认证的质量，建立统一的标准

可以提高行业的标准[4]。并且，国家认证是在政府的主导下进行数据安全认证，一般都会通过法律来保证实施，可以保证数据认证的规范性。然而，这种模式也有其不可避免的缺陷。在这种由政府统一认证的模式下，官僚主义和效率低下的问题是不可避免的。此外，政府所确立的高标准可能会将一部分小微企业阻挡在行业的大门外，不利于提高行业内部的活力。2018 年 3 月，法国 CNIL 决定放弃认证活动，并将其交给私人机构进行负责，也从侧面说明了国家认证的模式存在局限性。

2) 第三方认证

第三方认证是指由独立的社会组织来负责数据认证，通过制定自己的认证规则这一“软法”来约束行业内部数据处理的能力。这种模式可以根据不同的场景设计出不同的应对方式，此外因为其本身的独立性，体现出极其强烈的适应性，可以根据用户的要求进行调整。美国的网络隐私认证就是这种模式的典范。美国的网络隐私认证起始于上世纪 90 年代中后期，为了应对互联网经济这一新兴领域，在民间出现的一种自律形式。市场上主要有四家(TRUSTe、ESRB Privacy Online、WebTrust 以及 VeriSign)机构提供网络隐私印章。这种机构不仅能证明企业的数据保护能力是否达到标准，还能帮助解决关于网络隐私发生的纠纷。

第三方认证的优势以及局限性也是显而易见的，虽然其具有不同于国家认证的适应性，但也因为缺乏政府的监督，容易导致乱象的出现。比如认证机构之间的竞争的存在，会导致用户为了通过认证而寻找标准更低的机构进行认证。这种做法不仅不利于行业内部的数据处理能力的提高，而且会导致数据认证出现信任危机。

3) 自我声明

企业自我声明是由企业提供检测结果来声明自己的数据处理符合法定的标准的模式。美国联邦通信委员会(FCC)允许企业以这种方式来进行自证，可以使用电子标签，只需要保证产品文件中包含供应商符合性声明，不需要再向美国海关和边防局提供 FCC740 报关表格来证明自己符合标准。

这种模式虽然可以节省时间和其他成本，具有灵活性，但是这种模式仅靠自我约束，缺乏外部监督，很容易出现个人数据安全得不到保证的情况。并且这种自我声明因为成本的低廉，也很容易出现滥用的情形，使得可信度大大降低。

以上这三种模式从政府、社会、市场的角度出发，虽然都各有特色，但也各有利弊。国家认证的统一性是它的优势，但从成本和效率的角度来看确实难度颇高；自我认证的成本最低但由企业自我保护，认证的质量容易良莠不齐；第三方认证通过行业内部的社会机构来确保认证的标准，如果可以在政府的监管下进行公信力的保障，即政府监管下的第三方认证，这种模式既可以保留第三方认证的灵活性这一优点，同时也很好地获得了政府的公信力及资源的支持，可以获得一种相对的平衡。

(二) 欧盟《一般数据保护条例》的选择与实践

欧盟 GDPR 发展的趋势便是这种模式，在获批证书的机制下，由数据控制者获得确认数据处理操作符合《一般数据保护条例》的证书，是证明其数据处理的合法性和正确性的一种方法，这也是将个人数据传输至第三国，或者避免由监管部门处以罚款或减少罚款的手段。当然，这并不意味着自愿认证就可以免除数据控制者或者数据处理者遵守《一般数据保护条例》的义务，也不意味着它就限制了监管部门对那些已经证明了自己数据处理能力的数据处理者的监管权力。随着欧盟成员国国家法律的演进，出现了一种明显的趋势，就是将认证的权力委托给监管部门所认定的机构。认定这些机构的条款和方式将受到欧盟成员国国家的约束[4]。也就是说，GDPR 所建立的认证机制是由第三方认证机构实施认证程序并由各个成员国的数据保护机构进行监督的新机制。这种模式介于国家认证和纯粹的第三方认证之间，有效地保留了两种传统模式的优势，可以实现国家与社会的综合治理。

4. 我国数据安全认证的立法模式

随着数据安全在信息网络领域作用的日益凸显，我国的数据安全也在逐渐得到重视和发展。从 2019 年首次提出“建立数据保护能力认证机制”到 2022 年国家市场监督管理总局、国家互联网信息办公室联合发布的《关于开展数据安全管理认证工作的公告》(2022 年第 18 号文)及其附件《数据安全管理认证实施规则》(以下简称《规则》)正式落地，我国的数据安全认证逐渐走上了正轨。《规则》的内容明确规定了我国数据安全管理认证的模式、程序、证书、标志以及认证责任等事项，我国的安全管理认证制度(Date Security Management，以下简称 DSM)也因此建立。

DSM 选择的认证主体是网络运营者，从《规则》中的内容来看，我国的数据安全认证模式与 GDPR 的模式是殊途同归的，两者虽然在制度设计上存在着诸多不同之处，比如 GDPR 的认证对象是数据控制者或者数据控制者提供的产品、服务等，我国的认证主体则是符合技术规范和一定标准的数据安全管理体系，GDPR 的认证范围会更加广泛，涉及的对象也会更加丰富[5]。但是两者的共同点却是显而易见的，都将认证视为一种带有鼓励性质的激励制度，引导鼓励企业通过认证来提升数据处理能力和数据安全保障能力。

数据安全管理认证(DSM)首次以《GB/T41479-2022 信息安全技术网络数据处理要求》统一国内网络数据安全认证的标准，填补了国内关于数据安全标准的空白，为我国网络信息领域的治理添砖加瓦，促进了重要数据安全基础要素建设。

5. 数据安全认证的发展方向

目前我国数据安全管理制度虽然已经基本确立，但是具体的实施细则还未正式出台，具体的操作细则还需要进一步细化。数据安全认证机制的构建，是数字时代网络领域安全的探索，更深层反映的是传统政府职能的转变，是政府与社会合作治理的新模式。如何使数据认证模式的作用最大化，还需进一步探索。

(一) 保障数据安全认证规范及认证规则的科学性与专业性

数据安全认证是专业性极强的工作，其本身的属性要求认证的标准及认证程序必须严谨和专业。数据安全涉及国家、社会和个人等多个层面，当前网络领域的数据滥用现象种类多样且层出不穷，所以规范和制度的科学性就显得尤为重要。如果认证机构的专业度不够，那么就很难确保认证的权威性和可信度。欧盟《一般数据保护条例》第 43 条就对数据保护认证机构的专业性作出了要求，并明确列出了五项条件。因此，数据认证的具体规则在完善细化的过程中，应充分听取数据控制者、数据处理者、认证机构等多方意见。为了更加有效地进行数据安全认证，应不断提高认证机构的专业知识和技术水平，实现数据安全管理认证体系的优化建构。

(二) 落实数据认证机构的法律责任

一项制度的设定中如果缺少对法律责任的具体规定，那么实施一定会遇到阻力，规范本身的威慑力也会大打折扣。网络信息领域的数据认证是新兴领域，如果适用过于严苛的责任追究，势必会影响行业发展的积极性，但是如果放任不管，乱象丛生的环境也是不利于其发展和培育的[6]。认证机构的责任本身应该统一规定在《规则》之中，但是从目前的立法现状来看，还有待进一步细化。

(三) 加强数据安全认证国际合作与交流

虽然我国的数据安全管理的能力在不断提升，立法层面也在不断完善，但是与此同时，我国还应该尽快建立健全数据安全管理认证国际互认体系，打破壁垒，推动构建更加公平合理、开放包容、富有生机的网络空间。2022 年 11 月 7 日，国务院新闻办公室发布的《携手构建网络空间命运共同体》白皮书强调了网络空间命运共同体是信息时代的必然选择，同时也阐明了中国的贡献和主张。数据安全是个系统

性工程，需要各个环节、各个部门互相协助、互相配合，通力合作构建数据安全管理认证体系，为数字经济发展保驾护航。

6. 结语

数据安全认证体系的建立是网络空间领域的一个重要环节，对国家安全、个人数据保护都具有特别的价值。从域外的立法模式和实践应用来看，网络生态环境随着本土的现实各有不同，但是数据安全认证的可信度与声誉评价却是大家一致追求的目标。在大数据时代，网络信息高速发展的今天，如何在数字经济繁荣发展的同时确保个人信息的安全，是互联网行业的课题，也是国家治理体系中不可或缺的部分。

我国的数据安全认证体系尚在起步中，DSM 认证仍需不断地优化和打磨，需要在实践应用中找到应对网络信息安全的最优解。虽然数据安全认证不能解决互联网新兴领域出现的所有问题，但是它所具有的数据保护功能和商业价值是具有不可替代性的。虽然网络环境与技术标准等硬性条件会不断变化，但尊重个人信息安全的价值诉求和政府与社会多元合作的治理理念却是不会变的。

参考文献

[1] 张继红. 数据认证: 模式选择与应用规范[J]. 中国政法大学学报, 2021(2): 64-77.

[2] 刘懿阳. 《个人信息保护认证实施规则》背景下的认证制度实施[J]. 网络安全与数据治理, 2023, 42(1): 61-66.

[3] 张涛. 个人信息保护的整体性治理: 立法、行政与司法的协同[J]. 电子政务, 2023(6): 51-64.

[4] 刘权. 数据安全认证: 个人信息保护的第三方规制[J]. 法学评论, 2022, 40(1): 118-130.

[5] 段屹甲. 我国个人信息保护认证制度研究[D]: [硕士学位论文]. 江西: 江西财经大学, 2023

[6] 王玥, 方婷. 我国信息安全法律法规建设的基本原则与框架[J]. 中国信息安全, 2013(2): 43-46.